DOCUMENT RESUME

ED 472 807 CS 511 684

AUTHOR	Shyles, Leonard
TITLE	Authenticating, Identifying, and Monitoring Learners in the Virtual Classroom: Academic Integrity in Distance Learning.
PUB DATE	2002-11-00
NOTE	10p.; Paper presented at the Annual Meeting of the National Communication Association (88th, November 21-24, 2002, New Orleans, LA).
PUB TYPE	Guides - Non-Classroom (055) -- Opinion Papers (120) -- Speeches/Meeting Papers (150)
EDRS PRICE	EDRS Price MF01/PC01 Plus Postage.
DESCRIPTORS	*Cheating; *Distance Education; Higher Education; Proctoring; Student Behavior; Teacher Role
IDENTIFIERS	Biometrics; Monitoring

ABSTRACT

Cheating is not a problem unique to Internet-based training. It is a phenomenon that can and does compromise academic integrity in all settings, in both the traditional classroom and in distance-learning environments. But what are the remedies to compromises and abuses of the learning process, and challenges to the testing process in distance education? That is, how can distance education be administered so as to identify, authenticate, and monitor learners, minimize cheating, and thus maintain academic integrity? This paper proposes to provide an answer to this question. The paper discusses the virtual classroom, pointing out that the possibilities for abuse of academic integrity in the virtual classroom require special mechanisms to provide adequate monitoring in distance education. It notes the inevitability of distance education and contends that it is vital for institutions of higher learning that wish to remain in business to take the lead in developing systems that preserve academic integrity in the distance learning setting. The paper then describes some of the approaches to preserving academic integrity in the distance learning setting. In some cases, the approach is one that has been used for many years, while in other cases the approach is a relatively new but promising development. Includes 5 notes. (NKA)

Reproductions supplied by EDRS are the best that can be made
from the original document.

ED 472 807

Authenticating, Identifying, and Monitoring Learners in the Virtual Classroom: Academic Integrity in Distance Learning.

by Leonard Shyles

PERMISSION TO REPRODUCE AND DISSEMINATE THIS MATERIAL HAS BEEN GRANTED BY

L. Shyles

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

1

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

☐ This document has been reproduced as received from the person or organization originating it.

☐ Minor changes have been made to improve reproduction quality.

• Points of view or opinions stated in this document do not necessarily represent official OERI position or policy.

BEST COPY AVAILABLE

CS 511 684

AUTHENTICATING, IDENTIFYING, AND MONITORING LEARNERS IN THE VIRTUAL CLASSROOM: academic integrity in distance learning[1]

INTRODUCTION

The phrase *academic integrity* carries a variety of meanings. One meaning refers to the extent to which a course of learning that is offered actually delivers what it promises in a competent, clear, and complete way. Another meaning refers to the extent to which the assessment of student progress is carried out fairly, without bias, and ***without being compromised by dishonesty on the part of the test-taker—in short, without cheating.***

Cheating is not a problem unique to Internet-based training—it is a phenomenon that can and does compromise academic integrity in all settings, in both the traditional classroom and in distance-learning environments.[2] But what are the remedies to compromises and abuses of the learning process, and challenges to the testing process in distance education? That is, how can distance education be administered so as to identify, authenticate, and monitor learners, minimize cheating, and thus maintain academic integrity? Providing an answer to this question is the purpose of this report.

Potential compromises of academic integrity in distance learning

There are several ways in which academic integrity is traditionally open to abuse through cheating. One technique is for test-takers to have people that are not themselves take their tests for them (in short, through *impersonation* and *misrepresentation*). Another

---

[1] In fall 2001, the author was appointed to his university Task Force on Quality Control and Academic Integrity in Distance Learning. As part of that effort, the author attended a one-day conference workshop devoted to Identifying, Authenticating and Monitoring Learning on the Web hosted by the United States Army Distance Learning Program. This report is based in part on the proceedings and recommendations of that conference.

[2] In more than one study on cheating among high school students in America, the percentage of respondents who have admitted to serious test cheating has ranged from 74% to 97%.

technique is for test-takers to have outside help while engaged in test taking (either through *copying*, *communication*, or through *pre-knowledge* of examination content[3]). Copying includes secreting information containing test answers or relevant information in or near the test area so that it can be accessed during an examination.

The virtual classroom: a virtual certainty in the twenty-first century

The possibilities for abuse of academic integrity in the virtual classroom require special mechanisms to provide adequate monitoring in distance education. As the movement toward distance learning (also called distributed learning or distance education) progresses, and as more institutions of higher learning add distance learning courses to their traditional offerings, the development of effective remedies to compromises in academic integrity will become critical.[4] This is because failures to ensure academic integrity and quality control may over time erode institutional credibility, ultimately leading to challenges to accreditation, in addition to a loss of reputation among institutions with high academic standards.

At this writing, no one seriously questions the inevitability of distance education. Perhaps this is because training and testing in a distributed learning environment appears desirable for a number of reasons. First, it reduces costs for the learner who can "attend" class from home without having to travel. Second, it makes the lessons of master teachers available to the masses as never before. Third, it enables students in disparate locations to

---

[3] The techniques for cheating are highly varied. The technique of copying and engaging in communication can include the "wandering eye", where a test-taker simply glances at another's paper; or it can include hand signals, or the use of *M&Ms* candies color-coded to refer to specific multiple choice foils, or an endless variety of other coded messages. Pre-knowledge refers to test-takers smuggling databases into the test area and using them surreptitiously. Finally, impersonation refers to students using persons other than themselves take an exam for them. This form of cheating usually entails the use of fake Ids and other forms of misrepresentation.

[4] It is already clear that the Internet has increased the opportunities for academic integrity abuses through the sale of term papers and tests. Plagiarism is not a new phenomenon, but it has proliferated in recent years due to an increase in sources available through websites offering catalogs of term papers at a price.

share information and access materials at times convenient to them through asynchronous learning. In short, it enables students to acquire "anytime, anywhere education."

In addition, several studies have shown that distance learning in many cases works as well as face-to-face courses, is cost-effective in the long run, and results in student performance levels comparable to the traditional classroom setting. Further, some studies show that many different types of courses can be modified to accommodate distance learning needs, and that in many cases, it is possible for providers to affordably renovate their existing facilities to accommodate distance learning approaches. For these reasons, pervasive proliferation of distance education is only a matter of time. Therefore, it is vital for institutions of higher learning that wish to remain in business to take the lead in developing systems that preserve academic integrity in the distance learning setting.

The remainder of this report is devoted to describing some of the approaches to preserving academic integrity in the distance learning setting. In some cases, the approach is one that has been used for many years; in other cases, the approach is a relatively new but promising development.

PROCTORING to preserve academic integrity in distance learning

Even before students begin a course of study, they can be requested to sign a contract when they register for a course promising not to cheat. This may take place at the earliest stages of course registration. This is a *prevention* stage. At this stage, students may be asked to report to a proctoring center for course registration. Once there, they may be asked to write a paragraph describing what they expect to get out of the course, and what motivated them to enroll for the course etc. This material may be kept on file for later examination (i.e., to match handwriting with future test essays etc.). In addition,

students may be asked to pose for an image-capture photo-ID, for later verification at the time they take their exams.

At the examination stage (a *detection* stage), trained proctors may be used to count and secure all test materials at their proctoring station (stations may be located throughout the country where distance learning students may go to be tested). In such centers, a hotline may be set up for students who observe cheating to call to alert proctors that they believe cheating has occurred. The proctoring facility may also be furnished with a video camera. The students entering the area to take a test may be seated according to a seating chart by name. Standard proctoring procedures should be followed, including having all extraneous materials removed from the desks before test materials are distributed, and active monitoring of the test area for the duration of the exam by a proctor with a clear view of all examinees. With computer-based testing, some opportunities for cheating via copying are eliminated because question order can be randomized.

An *intervention* stage may follow, where materials may be crosschecked in instances where cheating may have occurred. In this stage, proctors or other examiners may search for unexplained irregularities, high score matches for students seated near one another, essay answers that appear to be in a completely different handwriting than the sample collected at the time of registration etc. If cheating is suspected, it is critical to have a remediation board to clear a score that is put in question. Remediation options for the student may include a re-test, a cancellation of the score, arbitration, a release of the file to an outside panel etc.

In summary, if a proctoring approach is used, it is essential to:

a) establish a policy in writing for handling examinations;

b) get an agreement in writing by the test taker;

c) keep materials secure;

d) appoint a test director to supervise the process;

e) train proctors;

f) document records in a central area.

BIOMETRIC SOLUTIONS for preserving academic integrity in distance learning

In addition to proctoring approaches, newly developing biometric approaches should be considered as possible alternatives for identifying and authenticating students in the distance learning setting, both for test-taking, and for determining the authenticity and authorship of course assignments (i.e., term papers).

Students in remote locations should be able to log on to participate in distance learning coursework, and to receive credit for work performed as part of a course requirement. But can a *public-key infrastructure* be trusted to secure the identity of a student at a remote location so that the work that is sent in for course credit can be determined with a high degree of certainty to be the product of the student claiming credit for the work that is produced? Some potential sources of abuse include plagiarism, collaboration, and outright cheating through misrepresentation (known as *bumping*[5]).

Currently digital passkeys, passwords, smart cards, and CD-ROM IDs are available to maintain a level of security for network users. But none of these approaches

[5] The term *bumping* refers to the practice of having a student seeking course credit sit down at a computer in a remote site, log on and provide the necessary password used to identify that student, and then getting up to permit an imposter to sit down and take an exam or provide some other material to be graded in the designated student's place.

can guarantee that distance learners who perceive a benefit from their abuse would not misuse these security measures. As verification techniques in the distance learning setting, these methods of securing files are inadequate. However, other verification methods are coming for authenticating student identity. These include *fingerprint, face recognition, handwriting, voice recognition,* and *iris scan* technologies, all of which use some measurable physical characteristic or personal behavioral trait of an individual to authenticate their identity.

When used properly, biometric techniques can offer a higher degree of assurance that individuals may be successfully identified in the distance learning setting. They offer enhanced security, accountability, and authentication capability.

However, it is a concern that if biometric data banks are accessible through a networked environment (i.e., over the Internet), then it is clearly possible that the integrity of the data base may be compromised by hackers, viruses etc. In such cases, it is critically important to encrypt the data to maintain security. Encryption techniques should also be used to protect the identities of individuals whose biometric information is stored in the system.

One approach being used to maintain the privacy of those whose information is in the database, is to store only *minutiae templates* rather than actual images of real fingerprints or iris scan information. What this means is that instead of storing an image of someone's fingerprint, a template is made of points of interest on an individual's fingerprint (in some systems, fifty or so points of interest are collected corresponding to places where peaks or whorls are located, and where other minute terrain features of a fingerprint are selected). Then the image of the actual fingerprint is discarded, and the

minutiae template is stored. In this way, the identity of the individual is masked, and the fingerprint is not part of the database. Then, when the student reports for an exam, he or she is asked to provide a thumbprint or iris scan again, and the same data points are collected so that a match can be made between the images. If they match, a successful identification has been made. In the case of iris scan technology, a minutiae template is collected in a 512-bit string, a huge improvement over the 4-character passwords used currently at ATM machines.

In terms of technical feasibility, minutiae templates require a much lower bandwidth than full imagery, and therefore are much faster and cheaper to administer than full image systems. In addition, tests of biometric scanning methods have yielded excellent results in terms of achieving high success rates. For example, the error rate associated with one system was 1 out of 1.2 million trials.

However, there are some legal and proprietary issues associated with biometric scanning techniques. For example, the *Americans with disabilities act* carries with it implications for consideration that may require an additional layer to the system at increased cost. Further, distributing enough systems nationwide can be expensive at the initial stages. Finally, even the most sophisticated systems are based on what is called an *asymmetric infrastructure*—that is, the success of such systems is ultimately based on 20 % technology, and 80% trust. In particular, the trust aspect refers to the need to maintain a database that must be placed in the hands of some trustworthy authority that must administer and handle the certification process that identifies a user with his or her file stored in the central database. In other words, all approaches to validating the authenticity of encrypted documents ultimately rely on a *certificate authority* that can match data

against a record on file. ***If the authority is corrupted, all bets are off***. For this reason, human trust and ethical action are elements of all systems, and these are ineluctable and irreducible features of biometric systems also.

From a practical perspective, at a minimum, biometric systems must be:

1) approved in terms of legal compliance;
2) low cost;
3) integrated with other aspects of the education system;
4) minimum bandwidth impact;
5) able to operate in varied field locations under varied circumstances and conditions;
6) outfitted with full encryption for all templates;
7) handicap accessible.

Subject: RE: NCA Conf/ ERIC Database submission CS 511 684
Date: Thu, 23 Jan 2003 08:13:11 -0500
From: "Ellis, Darra M" <dmellis@indiana.edu>
To: "Leonard Shyles" <leonard.shyles@villanova.edu>

Hello, thanks for your quick response! I printed your paper, but we need your actual signature on the release form. Please print it, sign it, and fax or mail to us. Thanks again.
Darra

-----Original Message-----
From: Leonard Shyles [mailto:leonard.shyles@villanova.edu]
Sent: Wednesday, January 22, 2003 5:18 PM
To: Ellis, Darra M
Subject: Re: NCA Conf/ ERIC Database submission

Dear Darra: Attached is the document you wanted. Feel free to use the below info as
you need to make this happen. If you need anything else from me, do not hesitate to
contact me.

Please confirm in an email that I have done all you need to get this to you. Best, Len
Shyles

PS> Thanks for you interest. I look forward to hearing from you .
Dear U.S. Department of Education
Office of Educational Research and Improvement (OERI)
National Library of Education (NLE)
Educational Resources Information Center (ERIC)

Reproduction Release (Specific Document)
I. DOCUMENT IDENTIFICATION:

Title: AUTHENTICATING, IDENTIFYING, AND MONITORING LEARNERS IN THE VIRTUAL CLASSROOM:
academic intergrity in distance learning
Author(s): Leonard Shyles
Corporate Source: Villanova University
Publication
Date: Spring 2002

II. REPRODUCTION RELEASE:
In order to disseminate as widely as possible timely and significant materials of interest
to the educational community,
documents announced in the monthly abstract journal of the ERIC system, Resources in
Education (RIE), are usually made
available to users in microfiche, reproduced paper copy, and electronic media, and sold
through the ERIC Document
Reproduction Service (EDRS). Credit is given to the source of each document, and, if
reproduction release is granted, one of the
following notices is affixed to the document.
If permission is granted to reproduce and disseminate the identified document, please
CHECK ONE of the following three
options and sign in the indicated space following.
The sample sticker shown below will be affixed
to all Level 1 documents

The sample sticker shown below will be affixed to all Level 2A documents

The sample sticker shown below will be affixed to all Level 2B documents

Level 1

Level 2A

Level 2B

Check here for Level 1 release, permitting reproduction and dissemination in microfiche or other ERIC archival media (e.g. electronic) and paper copy.

Check here for Level 2A release, permitting reproduction and dissemination in microfiche and in electronic media for ERIC archival collection subscribers only

Check here for Level 2B release, permitting reproduction and dissemination in microfiche only

Documents will be processed as indicated provided reproduction quality permits.

If permission to reproduce is granted, but no box is checked, documents will be processed at Level 1.

I hereby grant to the Educational Resources Information Center (ERIC) nonexclusive permission to reproduce and disseminate this document as indicated above. Reproduction from the ERIC microfiche, or electronic media by persons other than ERIC employees and its system contractors requires permission from the copyright holder. Exception is made for non-profit reproduction by libraries and other service agencies to satisfy information needs of educators in response to discrete inquiries.

Signature: Leonard Shyles

Printed Name/Position/Title: Len Shyles, Assoc. Prof., Department of Communication

Organization/Address: Villanova Unviersity

Telephone: 610 519 7923

Fax:

E-mail Address: Leonard.Shyles@villanova.edu

Date: Jan 22, 2003

III. DOCUMENT AVAILABILITY INFORMATION (FROM NON-ERIC SOURCE):

If permission to reproduce is not granted to ERIC, or, if you wish ERIC to cite the availability of the document from another source, please provide the following information regarding the availability of the document. (ERIC will not announce a document unless it is publicly available, and a dependable source can be specified. Contributors should also be aware that ERIC selection criteria are significantly more stringent for documents that cannot be made available through EDRS.)

Publisher/Distributor:
Address:

Price:

IV. REFERRAL OF ERIC TO COPYRIGHT/REPRODUCTION RIGHTS HOLDER:

If the right to grant this reproduction release is held by someone other than the addressee, please provide the appropriate name and address:
Name:
Address:

V. WHERE TO SEND THIS FORM:

Send this form to: ERIC Clearinghouse on Reading, English, and Communication (ERIC/REC).

ERIC/REC Clearinghouse | 2805 E 10th St Suite 140 | Bloomington, IN 47408-2698
Telephone: 812-855-5847 | Toll Free: 800-759-4723 | FAX: 812-856-5512
e-mail: ericcs@indiana.edu | WWW: http://eric.indiana.edu
EFF-088 (Rev. 9/97)

ERIC is a project of the U.S. Department of Education and the National Library of Education, with funding from the Office of Educational Research and Improvement (OERI).

ERIC/REC | Indiana University | Smith Research Center, Suite 140 | Bloomington, IN 47408-2698
(800) 759-4723 | (812) 855-5847 | FAX (812) 856-5512
System Administrator: Andy Wiseman | Database Administrator: Roger